I. Claims 1, 6, 11, and 21

Claims 1, 6, 11, and 21 were rejected under 35 USC § 102(b) as being anticipated by "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics" (Handley, et al.). This rejection is improper because the cited prior art does not teach "setting said packet TTL value to said smallest packet TTL value received for said corresponding packet flow." Three arguments are presented to show that this is the case.

Handley teaches several methods by which an attacker can evade detection by a network intrusion detection system (NIDS) by exploiting ambiguities (Pages 1-3). Handley then discloses a normalizer which is capable of altering packets to remove certain ambiguities to prevent these kinds of attacks from succeeding (Pages 3-15). In particular, one ambiguity that is discussed is the situation in which a packet arrives at a NIDS with a time-to-live (TTL) field too small to allow it to reach its destination (Page 2, Col. 1, item iii). A solution to this problem is presented according to which a packet normalizer increases the TTL of every incoming packet to a value large enough to ensure that every path within the protected network is reachable (Page 4, Col. 2, fourth paragraph and Page 9, Col. 1, at TTL solution #3).

The cited prior art does not teach "setting said packet TTL value to said *smallest packet TTL value received* for said corresponding packet flow" (emphasis added). The Office Action, on page 3, cites page 9, left column, TTL solution #3 of Handley as teaching this feature. The cited portion states:

> Configure the normalizer with a TTL that is larger than the longest path across the internal site. If packets arrive that have a TTL lower than the configured minimum, then the normalizer restores the TTL to the minimum.

(A)

The Office Action, on page 7, argues that restoring the TTL to the minimum is equivalent to setting said packet TTL value to said *smallest packet TTL value received* for said corresponding packet flow. However, **the "smallest**

packet TTL value received from each said corresponding packet flow" of claim 1 is not analogous to the configured minimum path across the internal site of Handley. Rather, in claim 1, clearly, the *smallest packet TTL value received* is the smallest TTL value of any packet received in a packet flow, which depends on all packets received (and analyzed) before the packet being processed. On the other hand, the configured minimum of Handley does not depend on any packets previously received – it is instead calculated based on the length of "the longest path across the internal site," which is invariant. Thus, the "smallest packet TTL value received from each said corresponding packet flow" of claim 1 is **not analogous** to the configured minimum path across the internal site of Handley.

(B)

The **method taught by Handley is inconsistent with the method of claim 1** because in claim 1, the setting has to be a decrease (based upon the language of the other limitations), while in Handley, the restoring of the TTL to the minimum inherently must be an increase.

In claim 1, each packet "belong[s] to a corresponding packet flow." Thus, inherent in the claim is the truth that for each packet being processed, the "smallest packet TTL value received from each said corresponding packet flow" cannot possibly be any larger than the TTL of that packet. Thus, "setting said packet TTL value to said *smallest packet TTL value received* for said corresponding packet flow" **can only result in the TTL value of that packet being maintained or decreased**.

However, in Handley, "**[i]f** packets arrive that **have a TTL lower** than the configured minimum, then the normalizer **restores the TTL to the minimum**." Thus, if a packet, upon being processed, has a TTL greater than or equal to the configured minimum, no action is taken (or at least, Handley does not teach what action is to be taken). **Only if the packet being processed has a TTL less than the configured minimum** does Handley teach that the normalizer alters the

TTL. Such **alteration then inherently takes the form of increasing the TTL** of the processed packet.

Thus, it would be **impossible** to perform the method of claim 1 in a way that would be anticipated by the cited portions of Handley.

(C)

Furthermore, **the method of claim 1 and the method of Handley clearly operate according to entirely different principles**. Handley prevents any packet with too small of a TTL from expiring before reaching its destination within a network. Thus, no retransmission packets will be needed. On the other hand, the method of claim 1 allows packets with a TTL that is too small to pass by, but since those packets will not be received by the end host, retransmission packets will be needed, so the method of claim 1 ensures that any retransmission packets will not have a TTL that is higher than that of the original packet.

Thus, Handley does not teach "setting said packet TTL value to said *smallest packet TTL value received* for said corresponding packet flow."

II. Claims 31, 33, 35, and 37

Claims 31, 33, 35, and 37 were rejected under 35 USC § 103(a) as being unpatentable over Handley in view of U.S. Patent Publication No. 2003/00095494 (McElligott). At the very least, this combination is not obvious, because the two references are directed to very different problems with very different solutions. Furthermore, the rationale provided by the Office Action to combine them does not appear to have any rational basis.

Handley is directed towards techniques for preventing attacks on a network through the use of a normalizer. McElligot, on the other hand, is directed to techniques for identifying the geographical location of a device. These fields are unrelated, and it is unclear why any person having ordinary skill in the art would be motivated to combine these references. The Office Action, on page 6,

presents an argument as to why a person having ordinary skill in the art would have combined Handley with McElligot, however, that argument does not actually explain why a person having ordinary skill in the art would be motivated to combine the references. Rather, it merely explains that McElligot teaches how to determine if the TTL is lower than a stored value. Thus, it would not have been obvious to a person having ordinary skill in the art at the time of the invention to have combined Handley with McElligot.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this effect is respectfully requested. Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, please charge any deficiency to Deposit Account No. 50-3661. If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

M. Ari Behar, Esq.
Attorney for Applicants
Registration No.: 58,203
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1004-128

Dated: April 8, 2009